A2 Cncld

further comprises: deriving a random initial vector from the string presented for verification; generating a sequence of unpredictable elements each of ℓ-bit length from the random initial vector in the same manner as used at signing method; and selecting n plaintext blocks from the string in the same order as that used at the signing method, and combining the selected plaintext blocks and the random vector with a different corresponding element of the sequence of unpredictable elements to obtain a plurality of input blocks, in the same manner as that used at the signing method.

<u>In the Claims</u>:

In accordance with 37 C.F.R. § 1.121(c)(1), please substitute for original claims 48, 53, 66, 72, 76 and 77, the following rewritten versions of the same claims, as amended. The changes made are shown explicitly in the attached "Version with Markings to Show Changes Made."

A3

48. (Amended) The method of claim 38, comprising:

generating said counter anew for every new key;

initializing generated counter to a constant value; and

for each message being signed using key, incrementing said counter by one; and

outputting said counter as an output block of the authentication scheme.

A4 Cm't

53. (Amended) The method as defined in claim 52, further comprising the steps of:

creating a secret random vector block of ℓ bits in length;

performing the same randomization function as that used at a signing method for determining an authentication tag over said plurality of plaintext blocks and the secret random vector block to create a plurality of input blocks each of ℓ bits in length;

wherein performing said randomization function further comprises:

deriving a random initial vector from said string presented for verification;

generating a sequence of unpredictable elements each of ℓ-bit length from said random initial vector in the same manner as used at signing method; and